American Institute of CPAs
1211 Avenue of the Americas
New York, NY 10036-8775

March 29, 2012

The Committee of Sponsoring Organizations of the Treadway Commission

Re: COSO Internal Control – Integrated Framework Exposure Draft

Dear COSO:

The American Institute of Certified Public Accountants (AICPA) is pleased to submit written comments on the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) exposure draft, *Internal Control – Integrated Framework* (the updated Framework).

The AICPA is the world's largest association representing the accounting profession, with nearly 377,000 members in 128 countries. AICPA members represent many areas of practice, including business and industry, public practice, government, and education; membership is also available to accounting students and CPA candidates. The AICPA sets ethical standards for the profession and U.S. auditing standards for audits of private companies, nonprofit organizations, and federal, state, and local governments. The AICPA also develops and grades the Uniform CPA Examination.

The comments herein reflect the views of the AICPA Internal Control Task Force, whose members represent business and industry, not-for-profit organizations, government organizations, and large, regional and local CPA firms.

We commend COSO for its efforts in updating the Framework. We believe that the updated Framework will continue to be an excellent and valuable resource to practitioners. We appreciate the opportunity to contribute the following comments which are addressed in response to COSO's request for feedback on the updated Framework. We changed the format of the statements in COSO's request for feedback to facilitate responding to them in this letter.

General Comments

We have found that too often in actual practice, users of the Framework view only control activities as actual controls and do not consider actions under the other four components to be "controls." Therefore, we recommend COSO consider including in the introduction that controls (e.g., process activities, policies and procedures) exist across all five components and across the entire entity, not only in the Control Activity component. Providing additional guidance in this area would be useful as some users of the updated

Framework continue to believe all controls are Control Activities and are not inherent in a process step or activity in the other components.

Within the updated Framework, there are various concepts (e.g., reasonable assurance, range of acceptability, and reducing risk of not achieving an objective to an acceptable level), as well as the notion of material weakness, which all relate to an effective system of internal control, but in slightly different ways. We believe the clarity and usefulness of the updated Framework would be enhanced if these concepts were tied together and appropriate examples provided.

We generally agree that the inclusion of the internal control principles and attributes provides helpful clarity to the various aspects of an effective system of internal control. However, we believe that their inclusion could increase the complexity of an organization's internal control evaluation process. We recommend COSO develop additional guidance related to how an organization should consider weaknesses in - or absence of - a principle or attribute when evaluating internal control effectiveness. In addition, we recommend COSO develop additional guidance in the following areas:

- Paragraph 77 of the updated Framework notes that a principle that is present and functioning operates within a "range of acceptability." However, we believe that the updated Framework lacks guidance regarding how organizations should consider ranges of acceptability in the development of its internal controls. We believe such guidance should include how a control's range of acceptability considers an organization's risk tolerance and reasonable assurance. In addition, we believe the guidance could be enhanced with examples illustrating the application of the "range of acceptability" concept.

- Paragraphs 88 and 89 of the updated Framework discuss the concepts of major non-conformity and minor non-conformity. Clarifying the examples to include which are considered a major vs. minor non-conformity and why would also help users better apply their judgment in their own evaluations.

- The updated Framework defines deficiencies in an organization's internal control over financial reporting differently from deficiencies in other components. For financial reporting deficiencies, the updated Framework incorporates the three tiers of deficiencies used by the SEC and the PCAOB related to external assessments required by Section 404 of the Sarbanes-Oxley Act of 2002. We recommend that COSO re-consider the incorporation of these concepts into the updated Framework, as we believe it unnecessarily links the updated Framework to a U.S. regulatory reporting framework and could risk obsolescence of the updated Framework based on future regulatory changes. We believe that it would be more appropriate for the updated Framework to consider deficiencies across all components consistently. To the extent further guidance tailored to the financial

> reporting component is deemed necessary, we believe that providing such guidance in COSO's upcoming external financial reporting guidance would be more appropriate for both public and nonpublic entities.

There seems to be some confusion by users of the current Framework between monitoring as a component of an internal control process and monitoring that might be required for regulatory or compliance purposes. If COSO intends there to be a difference, clarification is needed on the difference between monitoring as part of internal control and "monitoring" for purposes of supporting management's assertion about the effectiveness of an internal control process. We also recommend that the updated Framework more clearly describe or illustrate the differences between control activities and monitoring activities. For example, Paragraph 298 discusses control activities that operate more broadly and that typically take place at higher levels in the organization. It describes business performance or other analytical reviews, including actual performance versus budget, forecasts and prior periods and competitor results as examples. It also notes that the results of such reviews are analyzed and investigated and corrective actions are taken when results are not consistent with expectations. We note that the 2009 Monitoring Guidance refers to operating statistics, key risk indicators, key performance indicators and comparative industry metrics as providing indirect evidence that control are operating effectively. As such, we believe the discussion in paragraph 298, including the related examples, could better articulate the differences between control activities that operate at different levels of the organization and monitoring activities.

Changes to the Principles

The codification of the concepts from the original Framework into Principles is helpful to the users of the updated Framework. However, we believe the updated Framework would be enhanced if the below recommendations were considered.

The focus of Principle 8 is on fraud. We recommend that Principle 8 be expanded to include potential errors, bias and abuses, or alternatively an additional principle could be created under the Risk Assessment component. The expansion of the principle would make it clear that the risk of errors, bias and abuses are as important to assess as those related to fraud. These are the basic and more common risks that are present in all environments and often, in fact, are the more prevalent risks. We also believe the risk of management override should be more widely discussed and emphasized throughout the updated Framework. A more substantive discussion around this topic would provide greater context regarding a risk that often contributes to a deficiency in internal control. In addition to discussing management override as part of Risk Assessment, it would also be helpful for additional guidance, discussion, and examples to be included within the Control Environment chapter with respect to assessing, monitoring, and responding to the risk of management override.

Principle 10 covers specific activities which tend to monitor and/or mitigate specific risks to the achievement of objectives. Principle 11, on the other hand, appears to relate more to the control environment that needs to be in place so the board and management can be assured that specific control activities are working as intended and not being subverted. While we agree that general information technology controls are significant enough to warrant a separate principle, there is not enough clarity within the description to provide a user of the updated Framework sufficient understanding about how the two principles interact. Specifically, paragraph 295 could be enhanced to make it clear that automated controls are part of Principle 10 while Principle 11 addresses foundational concerns. Also, adding a description about the evaluation of the magnitude of a control deficiency or what would be considered as a significant deficiency in relation to Principle 11 may be helpful in clarifying the relationship between Principles 10 and 11.

Finally, we believe the meaning of the phrase "manifested in policies" as used in Principle 12 is unclear. We encourage COSO to clarify or modify this phrase. This could be achieved by modifying Principle 12 to state the following: *"The organization deploys control activities and related policies that establish what is expected and implements relevant procedures to affect the policies."*

Flexibility for Smaller Entities

The updated Framework notes that an organization's system of internal control will necessarily be different at a smaller organization as compared to a larger organization. However, we believe the updated Framework provides less emphasis on these differences than the original Framework, which included a discussion specific to each component focused on smaller organization implementation. We believe that this, combined with COSO's plans to supersede COSOs 2006 Guidance for Smaller Public Companies, may not provide smaller companies with sufficient perspective with respect to how the components and principles can be tailored to their particular facts and circumstances. In addition, we believe there are a number of areas within the updated Framework that may present particular challenges for smaller public and nonpublic organizations, including:

- Paragraph 143 states that "*it is necessary that the board contain outside directors*" and that "*it is important that the board contain at least a critical mass of outside directors*." While the updated Framework recognizes that not all smaller organizations will be able to comply with this requirement, it does not include alternatives to outside directors that would provide a comparable level of oversight. Moreover, other smaller organizations may lack a formal board governance structure altogether.

- While the updated Framework recognizes not all entities will have an internal audit department, in a number of instances, it appears to indicate that an internal audit (or similar) function is an integral part of an effective system of internal control. For example, paragraph 102 appears to indicate that a smaller organization would simply have a smaller internal audit function (or similar outsourced function) as compared to a larger entity. In addition, paragraph 154 characterizes internal audit as "*the third line of defense*" against the failure to achieve an entity's objectives. We believe that both of these discussions could be interpreted that an internal audit (or similar) function is necessary for an effective system of internal control, regardless of an organization's size.

Transition Guidance

Many organizations (both public and nonpublic) utilize the original Framework for compliance on internal control. While we understand that COSO does not intend to change the definition of effective internal control in the updated Framework, we believe that the codification of the principles and attributes may cause organizations to think differently regarding their conclusions regarding effectiveness. While we understand COSO is not a standard setting body, we believe that COSO should provide additional guidance with respect to transition to the updated Framework, including how users should consider the original Framework once the updated Framework is finalized. Such guidance could be in the form of recommendations to regulators and others that would be responsible for any official transition rules.

In Conclusion

We commend COSO on the work its done on the updated Framework. We believe that the updated Framework will continue to be an excellent and valuable resource to practitioners. While we believe that the updated Framework meets the objectives identified by COSO to enable organizations to effectively and efficiently develop and maintain systems of internal control that can enhance the likelihood of achieving the entity's objectives and can adapt to changes in the business and operating environments, it could be further improved by considering the points outlined in this letter.

On behalf of the AICPA and the members of the AICPA Internal Control Task Force, we appreciate the opportunity to comment on this exposure draft.

Sincerely,

William Schneider, CPA, CGMA
Chair, AICPA Internal Control Task Force

Susan S. Coffey, CPA, CGMA
Senior Vice President, Public Practice & Global Alliances